学术学位研究生培养方案

一级学科代码 　0839

一级学科名称 　网络空间安全

二级学科代码 　

二级学科名称 　

（☐博士点/☑硕士点，☐新增或计划新增学科）

此版培养方案自 2018 级研究生开始实施

青岛大学研究生院制表

2018 年 6 月 19 日

<table>
<tr><th colspan="2">一、学科研究方向及其特色和意义</th></tr>
<tr><td>研究方向</td><td>主要研究内容、特色和意义</td></tr>
<tr><td>密码学及应用</td><td>本学科方向主要涉及网络空间安全的关键技术--密码学以及在安全领域中的应用。密码学作为信息安全的关键技术，可以提供信息的保密性、完整性、可用性以及抗抵赖性。在密码学的研究领域，本学科方向的主要特色是侧重于密码技术的研究，考虑的是解决实际应用问题的密码方案的设计，研究的是信息安全中的共性技术。在信息安全诸多领域比如：大数据安全、云计算安全领域，都需要应用这些密码技术。在密码学应用的研究领域，本学科方向的主要特色是侧重于当前的新兴和热点领域中安全问题的解决。具体说来，本学科方向主要研究密码技术中的密钥泄露问题的解决方法、网络安全中的密钥管理协议、云存储中的完整性检测技术、云计算中的安全外包问题等。</td></tr>
<tr><td>网络与系统安全</td><td>网络安全是保障整个网络互连系统正常工作，提供多样化应用服务的基础，系统安全的特点是从系统级的整体上考虑信息安全的威胁与防护，二者相辅相成，有机统一，共同组成了网络空间安全领域的核心安全支撑体系。本学科方向的特色主要体现在数据库安全、可信网络体系与互连等几方面的研究工作上。在该领域与美国宾夕法尼亚州立大学、美国德州大学达拉斯分校等大学的研究机构进行了项目合作研究。在信息安全专业本科生和研究生教育环节，增加了该领域前沿技术理论介绍等课程内容。通过带领学生开展实践创新项目等形式，进一步培养学生的学习能力和实践能力。</td></tr>
<tr><td>安全算法理论</td><td>现代安全密码基础算法的研究大致可分为三类：Hash 函数、对称密码（私钥密码）算法与非对称密码（公钥密码）算法。本学科方向人员目前主要从事公钥密码算法的设计与安全性分析的理论研究。公钥密码的发展源于 1976 年 Diffie 与 Hellman 首次提出陷门单向函数思想实现加密密钥公开下的安全加密体制，奠定了公钥密码学的基础。公钥密码不仅可以提供信息的机密性，还提供认证功能，因此引起人们的高度关注并在计算机网络安全通信中广泛使用。公钥密码体制 RSA、ElGamal 体制、ECC 和 DSA 等成为公钥密码的标志性成果。尽管如此，新型公钥密码体制的设计与未来公钥密码体制的分析与攻击技术也不容忽视。1994 年，Shor 证明在未来量子计算机下，分解因子和离散对数问题是多项式时间可求解的。面对量子计算的高速发展与未来量子计算机的潜在威胁，设计抗量子计算的公钥密码算法被提升到一个前所未有的高度，已成为是国际密码领域重要研究内容。本学科方向的特色是研究安全算法的基础理论，特别是后量子密码基本理论，如：格上的困难问题，基于格的基本安全算法等。</td></tr>
<tr><td></td><td></td></tr>
</table>

二、培养目标

1、树立爱国主义和集体主义思想，掌握辩证唯物主义和历史唯物主义的基本原理，树立科学的世界观与方法论。具有良好的敬业精神和科学道德。品行优良、身心健康。

2、掌握坚实的网络空间安全的基础理论和系统的专门知识，了解学科的发展现状、趋势和研究前沿，较熟练地掌握一门外国语，具有良好的写作能力和国际学术交流能力；具有严谨求实的科学态度和作风，能够熟练运用网络空间安全学科的方法、技术与工具，从事该领域的基础研究、应用基础研究、关键技术及系统的分析、设计、开发与管理工作，具有从事本学科和相关学科领域的科学研究或独立担负专门技术工作的能力。

三、基本学习年限	学制 3 年，允许修业年限 2-6 年

四、培养方式及其他

1. 严格执行培养方案，采用导师负责、导师组集体培养相结合的方式因材施教培养研究生。充分发挥导师作用。成立导师组，会同有关教学系、学生管理部门对研究生的思想教育、学业与生活、科研工作等进行全面管理，保证培养质量。

2. 发挥导师、研究生两方面的积极性，研究生自学与导师指导相结合。

3. 坚持课程学习和学位论文工作并重。增强课程内容的前沿性，采用启发式、讨论式教学。理论课学习、科学研究、工程实践相结合，加强研究生实践能力的训练，培养网络空间安全技术与行业技术相结合的能力。

4. 重视对研究生进行系统性科研训练，以高水平科学研究支撑高水平研究生培养。支持研究生更多参与学术交流和国际合作，拓宽学术视野，激发创新思维。

五、本专业研究生课程设置及学分的基本要求

须修总学分 30 学分（含必修环节、必读书目 6 学分）

其中：学位课 17 学分、非学位课 7 学分

学术规范课、职业伦理课不少于 1 学分、创新创业类课不少于 1 学分

具体的课程设置如下：

类别	课程编号	课程名称	学分	学时	开课学期	开课院系	备注
公共学位课	4122001	中国特色社会主义理论与实践	2	32	1	马克思主义学院	
	4122003	自然辩证法概论（理工医科）	1	16	1	马克思主义学院	
	4052001	硕士英语综合	2	32	1	公共外语教育学院	
	4052002	硕士英语听说	2	32	1	公共外语教育学院	
专业学位课	4492001	计算机科学前沿讲座	1	16	1	计算机科学技术学院	考查
	4492101	网络空间安全数学基础	3	48	1	计算机科学技术学院	考试
	4492003	组合数学	3	48	1	计算机科学技术学院	考试
	4492102	密码学与网络安全	3	48	1	计算机科学技术学院	考试
专业非学位课	4492103	数据库安全	2	32	2	计算机科学技术学院	考查
	4492104	可证明安全密码理论	2	32	2	计算机科学技术学院	考查
	4492105	云计算安全技术	2	32	2	计算机科学技术学院	考查
	4492106	无线 Ad Hoc 网络安全	2	32	2	计算机科学技术学院	考查
	4492107	抗量子计算密码理论	2	32	2	计算机科学技术学院	考查
	4492108	区块链与数字货币原理	2	32	2	计算机科学技术学院	考查
	4492204	机器学习	2	32	2	计算机科学技术学院	考查
公共选修课	1052003	创新创业讲座	1	16	2	研究生院	网课(必选)
	1052004	科研诚信与学术规范	1	16	2	研究生院	网课(必选)
	1052002	信息检索（理）	1	16	2	研究生院	考查
	1052005	国际学术论文写作与发表	1	16	2	研究生院	网课
	1052006	研究生科研能力训练与培养	1	16	2	研究生院	网课
	4012001	日语	2	32	2	外语学院	
	4012002	法语	2	32	2	外语学院	
	4012003	朝鲜语	2	32	2	外语学院	

六、必修环节的基本要求（4 学分）
（一）实践活动的基本范围或基本形式（包括教学实践、医疗实践、社会实践、社会调查、科技开发和服务等内容的基本要求、工作量及考核方式）
实践活动　　　　　　　　　　　　　　2 学分 教学实践的内容可以是助教、助研、助管或指导本科生创新创业项目或论文等，课内外时数以 120 小时为宜，由学科负责安排。研究生应积极参加社会实践。每次活动均须撰写书面报告，填写《青岛大学研究生实践活动报告书》，内容包括思想小结、技术报告两部分，由导师或有关教师对其进行考核、给出评语和成绩。
（二）学术活动的次数、考核方式及基本要求（包括作学术报告、参加学术报告、前沿讲座，以及各种专题讨论班等内容的要求及考核方式）
学术活动　　　　　　　　　　　　　　2 学分 研究生须积极参加学术活动。每名研究生听取学术报告不少于 10 次、公开作学术报告不少于 2 次、撰写专业文献综述 1 篇，达到此要求方可获得学分。文献综述经导师签字后与开题报告一并交学院研究生工作秘书。

七、必读书目（本专业研究生须阅读的主要经典著作书目、专业学术期刊目录） （须完成不少于 20 篇阅读笔记，每篇不少于 1000 字）				
序号	著作或期刊的名称	作者或出版者	必读或选读	备　注
1	密码学原理与实践	Stinson[美]著，冯登国译，电子工业出版社	选读	
2	现代密码学理论与实践	Wenbo Mao 著，电子工业出报社	选读	
3	密码编码学与网络安全-原理与实践（第七版）	William Stallings（美）威廉·斯托林斯.王后珍 等译 电子工业出版社	必读	
4	IEEE Transactions on Dependable and Secure Computing	IEEE	选读	
5	IEEE Transactions on Information Forensics and Security	IEEE	选读	
6	Journal of Cryptology	Springer	选读	
7	ACM Transactions on Information and System Security	ACM	选读	
8	Computers & Security	Elsevier	选读	
9	Designs, Codes and Cryptography	Springer	选读	
10	Journal of Computer Security	IOS Press	选读	
11	ACM Conference on Computer and Communications Security （CCS）	ACM	选读	
12	International Cryptology Conference（CRYPTO）	Springer	选读	
13	European Cryptology Conference(EUROCRYPT)	Springer	选读	
14	IEEE Symposium on Security and Privacy (S&P)	IEEE	选读	
15	Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)	Springer	选读	
16	European Symposium on Research in Computer Security (ESORICS)	Springer	选读	
17	Journal of Computer Science and Technology	Springer	选读	

18	IEEE Communications Surveys and Tutorials	IEEE	选读	
19	International Workshop on Practice and Theory in Public Key Cryptography (PKC)	Springer	选读	
20	Theory of Cryptography Conference (TCC)	Springer	选读	
21	Workshop on Cryptographic Hardware and Embedded Systems (CHES)	Springer	选读	
22	The International Conference on Dependable Systems and Networks (DSN)	IEEE	选读	
23	Information and Computation	Elsevier	选读	
24	SIAM Journal on Computing	SIAM	选读	
25	IEEE Transactions on Information Theory	IEEE	选读	
26	计算机学报（中、英文版）	科学出版社	选读	
27	软件学报	科学出版社	选读	
28	中国科学（E 辑）	《中国科学》杂志社	选读	
29	中国密码学报	中国科学技术出版社	选读	
30	信息安全学报	科学出版社	选读	
31	信息网络安全		选读	

八、个人培养计划

根据专业培养方案、课题研究方向、研究生本人具体情况，研究生指导教师组织有关人员和研究生本人共同制定个人培养计划。培养计划应对学位课、选修课、各学期学分分配、考核方式和期限、教学实践、社会实践、学术活动、文献阅读、学位论文选题范围、论文预期目标及进度、科研工作等提出具体要求、做出具体安排。培养计划在硕士研究生入学后 6 周内制定，报研究生院备案。

九、开题、中筛工作的组织工作安排及要求

（开题、中筛工作的周期、组织形式等要求）

开题工作：最迟在第二学期末通过学位论文开题报告论证，通过者方可进入论文写作阶段。开题报告应公开进行，并由开题报告评议小组评审。硕士研究生开题评议小组由 3-5 名成员组成，均应具有副高以上职称，或具有硕士研究生指导教师资格。专家组成员对学位论文选题的创新性和可行性等进行重点评价，同时就论文工作提出具体意见和建议并给出结论。要制定具体的论文实施计划，由开题报告评议小组评审。评审通过后报学院学位评定委员会审核，并由学院存档。

中筛工作：一般在第四学期末进行学位论文中筛。中筛工作公开进行，并由中筛评议小组评审，小组由 3-5 名成员组成，均应具有副高以上职称，或具有硕士研究生指导教师资格。专家组对硕士研究生的中期总结报告进行评价，同时提出具体意见和建议并给出结论。参加考核的研究生填写《青岛大学研究生中期筛选考核表》，全面总结入学以来的思想、学习、科研等方面的情况。中期筛选的考核标准、内容、方法和结果处理按照《青岛大学关于对博士、硕士学位研究生实行中期筛选的暂行办法》实施。

十、学位论文工作的内涵要求

（包括开题、中筛、预答辩的学术水平和研究生工作量要求）

学位论文是研究生培养的重要环节，研究生在修完学位课程并完成规定学分后，可以开展学位论文工作。研究生在导师或导师组指导下完成学位论文，导师为第一责任人，对论文质量全程把关。论文工作包括论文选题、开题报告、中期检查、论文撰写、论文答辩等几个环节。撰写学位论文要坚持理论与实践结合的原则，论文课题应具理论意义和实际意义相结合。研究生从事与学位论文有关的研究工作不少于 1 年时间。

（一）论文开题

研究生在撰写学位论文前应阅读大量中外文献资料，在了解主攻方向历史和现状的基础上确定论文题目、写出开题报告。进入论文工作前，须在查阅文献、调查研究的基础上进行开题报告，由教研室或学科点组织审定。开题报告内容包括：选题意义、文献综述（不少于 8000 字）、研究计划及目标、主要技术（理论）难点及拟解决方案等。

（二）论文中筛

为确保研究生按期完成高质量的学位论文，应于第四学期组织有关人员就研究生论文工作情况进行全面检查和阶段性总结。学院组织考核小组，对研究生的综合能力、论文工作进展情况以及工作态度和精力投入等进行全面考核。中期考核的目的在于关注论文工作进展，及时给予指导。

（三）论文预答辩

学位论文完成后，在正式答辩之前需要进行预答辩，考察论文的完成情况。学位论文必须由研究生独立完成，合作项目应明确其本人为主完成的部分。学位论文内容应包括课题背景、国内外研究动态、设计方案的比较与评估、需要解决的主要问题和途径、本人在课题中所做的工作、理论分析、分析设计、测试装置和试验手段、试验数据处理、必要的图纸、图表曲线与结论、结果的技术和经济效果分析、所引用的参考文献等。与他人合作或前人基础上继续进行的课题，必须在论文中明确指出本人所做的工作。学位论文完成后，由学科按规定程序组织论文评阅和答辩，提出是否授予学位的意见，并将所有申报材料整理好，由学院学位评定委员会主席签字（一式三份）后上报学校学位评定委员会审批。

十一、毕业和学位授予要求

完成个人培养计划，达到学科培养方案规定的各环节要求，完成学位论文工作，通过学位论文答辩，颁发硕士研究生毕业证书。

为保证学位授予质量，在申请硕士学位前，研究生需达到经校学位办备案的、学院（学部）自主制定的硕士学位申请学术条件，并符合《青岛大学博士、硕士学位授予工作细则》有关规定，经学校审核通过，授予相应硕士学位。

其　　它　　说　　明
无 本学科（或二级学科）负责人签名：[签名] 2018年6月20日
所在院系意见： 同意 负责人（签名）：[签名] （加盖学院公章） 2018年6月21日
一级学科专家组（或院系研究生教育指导委员或学位评定分委员会）验收意见： 同意 负责人（签名）：[签名] 2018年6月21日